

JAN 21 2009
FCC Mail Room

EB Docket No. 06-36

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street S.W., Suite TW-A325
Washington, D.C. 20554

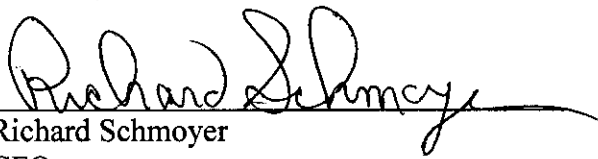
Dear Secretary Dortch,

In accordance with 47 CFR 64.2009(e), please find attached the Company's Annual Compliance Certificate for the previous calendar year, 2008. The Compliance Certificate includes the Company's:

- Statement explaining how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

If you have any questions regarding this filing, please direct them to the undersigned.

Sincerely,


Richard Schmoyer
CFO

Enclosure

cc: Federal Communications Commission, Enforcement Bureau,
Telecommunications Consumers Division, 445 12th Street SW, Washington, DC
20554 (2 courtesy copies)

Best Copy and Printing, Inc., FCC@BCPIWEB.COM

No. of Copies rec'd 0
List ABCDE

CERTIFICATE OF COMPLIANCE WITH PROTECTION OF CUSTOMER PROPRIETARY NETWORK INFORMATION RULES

Including:

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

Explanation of Any Actions Against Data Brokers, and

Summary of all Customer Complaints Received

Paul Bowman signs this Certificate of Compliance in accordance with § 222 of the Telecommunications Act of 1996, as amended, 47 USC 222, and 47 CFR 64.2009, on behalf of Comlink, LLC., related to the previous calendar year, 2008.

This Certificate of Compliance addresses the requirement of 47 CFR 64.2009 that the Company provide:

- A "statement accompanying the certificate" to explain how its operating procedures ensure compliance with 47 CFR, Part 64, Subpart U;
- An explanation of any actions taken against data brokers; and
- A summary of all customer complaints received in the past year concerning the unauthorized release of customer proprietary network information (CPNI).

On Behalf Of The Company, I Certify As Follows:

1. I am the President of the Company, and therefore an officer of the Company. My business address is 1515 Turf Lane, Suite 100, East Lansing, Michigan 48823. The Company's Form 499 Filer ID is 826877.

2. I have personal knowledge of the facts stated in this Certificate of Compliance. I am responsible for overseeing compliance with the Federal Communications Commission's (FCC) rules relating to CPNI.

Statement Explaining How Operating Procedures Ensure Regulatory Compliance

3. I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the FCC's regulations governing CPNI, including those adopted on March 13, 2007 in CC Docket No. 96-115.

4. The Company ensures that it is in compliance with the FCC's CPNI regulations. The Company trains its personnel regarding when they are authorized to use CPNI, when they are not authorized to use CPNI, and how to safeguard CPNI. The Company maintains a CPNI Compliance Manual in its offices for purposes of training of new and current employees, and as a reference guide for all CPNI issues. Our CPNI Compliance Manual is updated to account for changes in law, including the FCC's most recent changes to its regulations governing CPNI, adopted on March 13, 2007 in CC

Docket No. 96-115. The CPNI Manual contains key all essential information and forms to ensure the Company's compliance with CPNI regulations.

5. The Company has established a system by which the status of a Customer's approval for use of CPNI, as defined in 47 USC 222(h)(1), can be clearly established prior to the use of CPNI. The Company relies on the involvement of its high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

6. Company personnel make no decisions regarding CPNI without first consulting with management.

7. The Company has an express disciplinary process in place for personnel who make unauthorized use of CPNI.

8. The Company's policy is to maintain records of its own sales and marketing campaigns that use CPNI. The Company likewise maintains records of its affiliates' sales and marketing campaigns that use CPNI. The Company also maintains records of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records in its offices for a minimum of one year.

9. In deciding whether the contemplated use of the CPNI is proper, management consults one or more of the following: the Company's own compliance manual, the applicable FCC regulations, and, if necessary, legal counsel. The Company's sales personnel must obtain supervisory approval regarding any proposed use of CPNI.

10. Further, management oversees the use of opt-in, opt-out, or any other approval requirements, or notice requirements (such as notification to the Customer of the right to restrict use of, disclosure of, and access to CPNI), contained in the FCC's regulations. Management also reviews all notices required by the FCC regulations for compliance therewith. Before soliciting for approval of the use of a Customer's CPNI, the Company will notify the Customer of his or her right to restrict use of, disclosure of, and access to, his or her CPNI.

11. The Company maintains records of Customer approval and disapproval for use of CPNI in a readily-available location that is consulted on an as-needed basis.

12. The Company complies with all FCC requirements for the safeguarding of CPNI, including use of passwords and authentication methods, and the prevention of access to CPNI (and Call Detail Information in particular) by data brokers or "pre-texters."

13. The Company, on an ongoing basis, reviews changes in law affecting CPNI, and updates and trains company personnel accordingly.

Explanation of Actions Against Data Brokers

14. The Company has not encountered any circumstances requiring it to take any action against a data broker during the year to which this Certificate pertains.

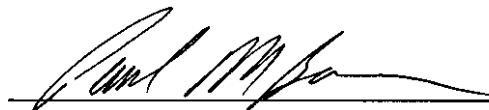
Summary of all Customer Complaints Received

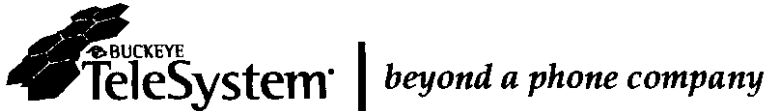
15. The following is a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI: None.

16. The Company does not at this point have any specific information on the processes pretexters are using to attempt to access its Customer's CPNI.

Date: _____

1/12/09

 CEO



www.buckeye-telesystem.com

Received & Inspected

JAN 21 2009

FCC Mail Room

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW Ste TW-A235
Washington, DC 20544

**RE: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: Jan. 15, 2009

Name of company(s) covered by this certification: Buckeye Telesystem, Inc.

Form 499 Filer ID: 817466

Name of signatory: Joe Jensen

Title of signatory: President

I, Joe Jensen, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed 

Copy: Best Printing

No. of Copies rec'd 0
List ABCDE

EXHIBIT A
Buckeye Telesystem, Inc.

These policies and procedures, which are briefly summarized below, ensure compliance by limiting access to, use of, and disclosure of CPNI.

Only authorized personnel can access CPNI. All personnel so authorized, such as customer service representatives and billing and collection personnel, are trained in the appropriate access to, use of, and disclosure of CPNI. Failure to abide by the applicable policies and procedures is cause for discipline, up to and including termination.

The Company does not share CPNI among its affiliates other than in direct support of its business, unless prior customer approval has been obtained or no customer approval is needed. Further, the Company requires all independent contractors who have access to CPNI to enter an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as requested by the customer or as compelled or authorized by law.

The Company has always and will always require the customer to choose a password when establishing a service account.

The Company notifies customers of their right to restrict access to, use of, and disclosure of their CPNI annually through bill inserts. The Company maintains records of all customer requests to opt-out of any communication or related disclosure for all communication other than in direct support of the Company's business.

All out-bound marketing campaigns that utilize CPNI are subject to managerial approval and to verification of customer approval to use CPNI in this manner. Records related to such efforts are maintained for at least one year.

Managerial personnel monitor access to, use of, and disclosure of CPNI on an on-going basis to ensure compliance with the applicable policies and procedures and to evaluate their effectiveness. The Company will report to the Commission instances, if any, in which opt-out mechanisms do not work properly.

DO NOT FILE COPY ORIGINAL



Buckeye CableSystem

Executive Offices
5555 Airport Highway, Suite 110
Toledo, Ohio 43615

419.724.9802

Received & Inspected

JAN 21 2009

FCC Mail Room

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW Ste TW-A235
Washington, DC 20544

**RE: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: Jan. 15, 2009

Name of company(s) covered by this certification: Buckeye Cablevision, Inc.

Form 499 Filer ID: NA

Name of signatory: W.H. "Chip" Carstensen

Title of signatory: President and General Manager

I, W.H. "Chip" Carstensen, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Copy: Best Printing

No. of Copies rec'd 0
List ABCDE

EXHIBIT A
Buckeye Cablevision, Inc.

These policies and procedures, which are briefly summarized below, ensure compliance by limiting access to, use of, and disclosure of CPNI.

Only authorized personnel can access CPNI. All personnel so authorized, such as customer service representatives and billing and collection personnel, are trained in the appropriate access to, use of, and disclosure of CPNI. Failure to abide by the applicable policies and procedures is cause for discipline, up to and including termination.

The Company does not share CPNI among its affiliates other than in direct support of its business, unless prior customer approval has been obtained or no customer approval is needed. Further, the Company requires all independent contractors who have access to CPNI to enter an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as requested by the customer or as compelled or authorized by law.

The Company has always and will always require the customer to choose a password when establishing a service account.

The Company notifies customers of their right to restrict access to, use of, and disclosure of their CPNI annually through bill inserts. The Company maintains records of all customer requests to opt-out of any communication or related disclosure for all communication other than in direct support of the Company's business.

All out-bound marketing campaigns that utilize CPNI are subject to managerial approval and to verification of customer approval to use CPNI in this manner. Records related to such efforts are maintained for at least one year.

Managerial personnel monitor access to, use of, and disclosure of CPNI on an on-going basis to ensure compliance with the applicable policies and procedures and to evaluate their effectiveness. The Company will report to the Commission instances, if any, in which opt-out mechanisms do not work properly.

Our family serving your family

Skyline Telephone

2205 Keithley Creek Road

P. O. Box 10

Midvale, ID 83645

Received & Inspected

JAN 21 2009

FCC Mail Room

Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date of execution: January 15, 2009

Name of Company covered by this certification: Skyline Telephone Company

Form 499 Filer ID: 821312

Name of Officer signing: Lane R. Williams

Title of Officer signing: President

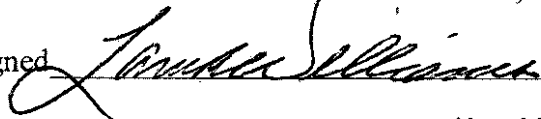
I, Lane R. Williams, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification as Exhibit 1 is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any acitons (proceedings instituted or petitions filed by a company at either state commission, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer-complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed



No. of Copies rec'd
List ABCDE

0

1-208-355-2580 (office)

1-888-782-4680

1-208-355-2222 (fax)

1-509-556-2000 (service)

SKYLINE TELEPHONE COMPANY

**STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES
ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES**

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

II. Use and Disclosure of CPNI Is Restricted

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use the Company's CPNI, the agent's, independent contractor's or joint venture partner's agreement with the Company must contain provisions (or the Company and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) the agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the Company's CPNI.

III. Protection of CPNI

1. The Company may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address or record. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.
2. The Company will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.
3. The Company retains all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.
4. Company employees authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, Company employees must: (a) be furnished the customer's pre-established password (or correct answers to the back-up "shared secret" combinations); (b) send the requested information to the customer's postal or electronic "address of record" (see definition above); or (c) call the customer back

at the customer's "telephone number of record" (see definition above) with the requested information.

5. If a customer subscribes to multiple services offered by the Company and an affiliate, the Company is permitted to share the customer's CPNI regarding such services with its affiliate. If a customer does not subscribe to any telecommunications or non-telecommunications services offered by an affiliate, the Company is not permitted to share the customer's CPNI with the affiliate without the customer's consent pursuant to the appropriate notice and approval procedures set forth in Sections 64.2007, 64.2008 and 64.2009 of the FCC's Rules.

6. When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

The Company discloses or releases call detail information to customers during customer-initiated telephone contacts only when the customer provides a pre-established password. If the customer does not provide a password, call detail information is released only by sending it to the customer's address of record or by the carrier calling the customer at the telephone number of record. If the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.)

7. The Company uses, discloses, and/or permits access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing) only pursuant to the notice and approval procedures set forth in Sections 64.2007, 64.2008, and 64.2009 of the FCC's Rules. All proposed out-bound marketing activities are reviewed by the Company's CPNI Compliance Officer for compliance with the CPNI restrictions and requirements in the Communications Act and the FCC Rules.

8. The Company maintains appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status of each customer's Out-out and/or Opt-In approvals (if any) prior to use of the customer's CPNI. These records include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

9. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, the Company's records must be checked to determine the status of the customer's CPNI approval. Company employees, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records.

If new, additional or extended approvals are necessary, the CPNI Compliance Officer will determine whether the Company's "Opt-Out CPNI Notice" or "Opt-In CPNI Notice" must be used with respect to various proposed out-bound marketing activities.

10. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign; and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of one year.

11. The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

12. The Company's employees and agents may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

13. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may the Company's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

14. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

15. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

16. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

17. The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account. Passwords may NOT be based upon readily obtainable biographical information (*e.g.*, the customer's name, mother's maiden name, social security number or date of birth) or account information (*e.g.*, the customer's telephone number or address).

18. Customers may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their telephone number of record, and then wait at that number until a Company representative calls them back and obtains correct answers to certain questions regarding their service and address.

19. The Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a Company call or voicemail to the customer's telephone number of record; (b) a Company text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

d. The Company employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing: (a) the name, address of record, and telephone number of record of the customer notified; (b) a copy or the exact wording of the text message, written notice, telephone message or voicemail message comprising the notice; and (c) the date and time that the notice was sent.

20. The Company must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

a. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide electronic notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC at <http://www.fcc.gov/eb/cpni>.

21. The Company will provide customers with access to CPNI at its retail locations if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

22. The Company takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees, agents, independent contractors and joint venture partners to notify the CPNI Compliance Officer immediately by voice, voicemail or email of: (a) any suspicious or unusual call requesting a customer's call detail information or other CPNI (including a call where the caller furnishes an incorrect password or incorrect answer to one or both of the "shared secret" question-answer combinations); (b) any suspicious or unusual attempt by an individual to change a customer's password or account information (including providing inadequate or inappropriate identification or incorrect "address or record," "telephone number of record" or other significant service information); (c) any and all discovered instances where access to the Company's electronic files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and (d) any complaint by a customer of unauthorized or inappropriate use or disclosure of his or her CPNI. The CPNI Compliance Officer will request further information in writing, and investigate or supervise the investigation of, any incident or group of incidents that reasonably appear to entail pretexting.

23. **[CMRS carriers subject to E911 location requirements only; others delete]** The Company and its authorized employees may use CPNI to provide call location information regarding mobile users in certain emergency situations. Except in an unforeseen emergency involving a substantial threat to human life or safety, any and all use or provision of CPNI under this category must involve the specific types or categories of emergencies listed in writing by the Company's CPNI Compliance Officer.

IV. CPNI Compliance Officer

In addition to the specific matters required to be reviewed and approved by the Company's CPNI Compliance Officer, employees and agents, independent contractors and joint venture partners are strongly encouraged to bring any and all other questions, issues or uncertainties regarding the use, disclosure, or access to CPNI to the attention of the Company's CPNI Compliance Officer for appropriate investigation, review and guidance. The extent to which a particular employee or agent brought a CPNI matter to the attention of the CPNI

Compliance Officer and received appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure or access to CPNI.

V. Disciplinary Procedures

The Company has informed its employees and agents, independent contractors and joint venture partners that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by Company employees or agents of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious).

Violation by Company independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training and termination of the contract).

SKYLINE TELEPHONE COMPANY

STATEMENT OF ACTIONS TAKEN AGAINST DATA BROKERS

- A. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

- B. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Idaho, Arizona and Oregon Commissions:

NONE

- C. During Calendar Year 2008, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following federal or state courts:

NONE

SKYLINE TELEPHONE COMPANY

**SUMMARY OF CUSTOMER COMPLAINTS
REGARDING UNAUTHORIZED RELEASE OF CPNI**

- A. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees:

NONE

- B. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

- C. During Calendar Year 2008, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

- D. During Calendar Year 2008, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE



Buckeye CableSystem

Erie County Cablevision, Inc.

DOCKET FILE COPY ORIGINAL

Received & Inspected

JAN 21 2009

FCC Mail Room

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW Ste TW-A235
Washington, DC 20544

**RE: Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2008

Date filed: Jan. 15, 2009

Name of company(s) covered by this certification: Erie County Cablevision, Inc.

Form 499 Filer ID: NA

Name of signatory: Patrick Deville

Title of signatory: President and General Manager

I, Patrick Deville, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Copy: Best Printing

No. of Copies rec'd 0
List ABCDE

EXHIBIT A
Erie County Cablevision, Inc.

These policies and procedures, which are briefly summarized below, ensure compliance by limiting access to, use of, and disclosure of CPNI.

Only authorized personnel can access CPNI. All personnel so authorized, such as customer service representatives and billing and collection personnel, are trained in the appropriate access to, use of, and disclosure of CPNI. Failure to abide by the applicable policies and procedures is cause for discipline, up to and including termination.

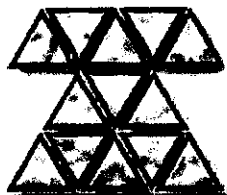
The Company does not share CPNI among its affiliates other than in direct support of its business, unless prior customer approval has been obtained or no customer approval is needed. Further, the Company requires all independent contractors who have access to CPNI to enter an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as requested by the customer or as compelled or authorized by law.

The Company has always and will always require the customer to choose a password when establishing a service account.

The Company notifies customers of their right to restrict access to, use of, and disclosure of their CPNI annually through bill inserts. The Company maintains records of all customer requests to opt-out of any communication or related disclosure for all communication other than in direct support of the Company's business.

All out-bound marketing campaigns that utilize CPNI are subject to managerial approval and to verification of customer approval to use CPNI in this manner. Records related to such efforts are maintained for at least one year.

Managerial personnel monitor access to, use of, and disclosure of CPNI on an on-going basis to ensure compliance with the applicable policies and procedures and to evaluate their effectiveness. The Company will report to the Commission instances, if any, in which opt-out mechanisms do not work properly.



MIDVALE TELEPHONE EXCHANGE, INC.

Serving Rural Customers in Idaho, Arizona, Oregon & Washington
 2205 KEITHLEY CREEK ROAD • P.O. BOX 7 • MIDVALE, IDAHO 83645
 (208) 355-2211 1-800-462-4523 FAX (208) 355-2222

Received & Inspected

JAN 21 2009

FCC Mail Room

Marlene H. Dortch, Secretary
 Federal Communications Commission
 445 12th Street, SW
 Washington, DC 20554

Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2008
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date of execution: January 15, 2009

Name of Company covered by this certification: Midvale Telephone Exchange, Inc.

Form 499 Filer ID: 803682

Name of Officer signing: Lane R. Williams

Title of Officer signing: President

I, Lane R. Williams, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification as Exhibit 1 is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company has not taken any acitons (proceedings instituted or petitions filed by a company at either state commission, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

www.midvaletelephone.com
Family Owned Since 1943

No. of Copies rec'd _____
 List ABCDE _____

MIDVALE TELEPHONE EXCHANGE, INC.

**STATEMENT EXPLAINING HOW THE COMPANY'S OPERATING PROCEDURES
ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES**

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information).

Generally, CPNI includes personal information regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

II. Use and Disclosure of CPNI Is Restricted

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company.

The Company has designated a CPNI Compliance Officer who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized to use or access the Company's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use the Company's CPNI, the agent's, independent contractor's or joint venture partner's agreement with the Company must contain provisions (or the Company and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) the agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the Company's CPNI.

III. Protection of CPNI

1. The Company may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address or record. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.

2. The Company will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.

3. The Company retains all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.

4. Company employees authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, Company employees must: (a) be furnished the customer's pre-established password (or correct answers to the back-up "shared secret" combinations); (b) send the requested information to the customer's postal or electronic "address of record" (see definition above); or (c) call the customer back

at the customer's "telephone number of record" (see definition above) with the requested information.

5. If a customer subscribes to multiple services offered by the Company and an affiliate, the Company is permitted to share the customer's CPNI regarding such services with its affiliate. If a customer does not subscribe to any telecommunications or non-telecommunications services offered by an affiliate, the Company is not permitted to share the customer's CPNI with the affiliate without the customer's consent pursuant to the appropriate notice and approval procedures set forth in Sections 64.2007, 64.2008 and 64.2009 of the FCC's Rules.

6. When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if the Company provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after the Company authenticates the customer.

The Company discloses or releases call detail information to customers during customer-initiated telephone contacts only when the customer provides a pre-established password. If the customer does not provide a password, call detail information is released only by sending it to the customer's address of record or by the carrier calling the customer at the telephone number of record. If the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (*i.e.*, the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.)

7. The Company uses, discloses, and/or permits access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing) only pursuant to the notice and approval procedures set forth in Sections 64.2007, 64.2008, and 64.2009 of the FCC's Rules. All proposed out-bound marketing activities are reviewed by the Company's CPNI Compliance Officer for compliance with the CPNI restrictions and requirements in the Communications Act and the FCC Rules.

8. The Company maintains appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status of each customer's Out-out and/or Opt-In approvals (if any) prior to use of the customer's CPNI. These records include: (i) the date(s) of any and all of the customer's deemed Opt-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

9. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, the Company's records must be checked to determine the status of the customer's CPNI approval. Company employees, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records.

If new, additional or extended approvals are necessary, the CPNI Compliance Officer will determine whether the Company's "Opt-Out CPNI Notice" or "Opt-In CPNI Notice" must be used with respect to various proposed out-bound marketing activities.

10. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign; and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of one year.

11. The Company's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Company's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

12. The Company's employees and agents may use CPNI without customer approval to protect the Company's rights or property, and to protect users and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived.

Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved in advance and in writing by the Company's CPNI Compliance Officer.

13. The Company's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may the Company's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

14. Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

15. Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

16. Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

17. The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account. Passwords may NOT be based upon readily obtainable biographical information (*e.g.*, the customer's name, mother's maiden name, social security number or date of birth) or account information (*e.g.*, the customer's telephone number or address).

18. Customers may obtain an initial or replacement password: (i) if they come in person to the Company's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified Company telephone number from their telephone number of record, and then wait at that number until a Company representative calls them back and obtains correct answers to certain questions regarding their service and address.

19. The Company will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a Company call or voicemail to the customer's telephone number of record; (b) a Company text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

d. The Company employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing: (a) the name, address of record, and telephone number of record of the customer notified; (b) a copy or the exact wording of the text message, written notice, telephone message or voicemail message comprising the notice; and (c) the date and time that the notice was sent.